

Information Services & Technology (IS & T)

Summary of Information Request

This information is the property of the Division of Credit Unions and is received from the credit union for our confidential use.

Under no circumstances may any recipient of this examination information use, disclose, or make it public except as authorized relating to credit union regulation. The law provides penalties for unauthorized use or disclosure of any such information, which is not otherwise publicly available. If any subpoena or other legal process is received calling for the production of such information, you should notify the DCU immediately.

General Directions

Reports and information should be prepared as of the exam cutoff date. Management may wish to discuss individual credit union report options with the Examination Supervisor or the EIC examiner prior to the exam start. **If you cannot provide the documents or answers requested, please indicate why. If a particular question is not applicable, simply indicate N/A.**

Supporting Documentation

Some questions in the EC-1 questionnaire require supporting documentation in order to verify the response given. For each of the major sections of the EC-1 questionnaire, examples of supporting documentation are listed below. To the extent appropriate, please have this documentation available for the examiners.

Section 1. General:

- 1.1. Please complete the attached EC-1 Questionnaire
- 1.2. Provide all written policies and procedures that relate to information technology management, E-commerce, electronic delivery systems, and information technology security
- 1.3. Board packets for the most recent 12 months, including reports from the Supervisory Committee and any other committees involved in technology initiatives
- 1.4. a) Credit Union organizational charts, including b) IT and E-Commerce departments
- 1.5. Copies of any strategic or business plans related to technology initiatives

Section 2. Risk Assessment

- 2.1. a) Risk Assessments of E-Commerce, Information Technology and related activities. b) Include any responses and evidence of corrective actions.

Section 3. Compliance and Legal

- 3.1. a) Legal opinions or b) other related correspondence from counsel related to E-Commerce.

- 3.2. a) Most recent insurance coverage review and b) recommendations performed by the bonding company, as well as a c) copy of the current bond policy

Section 4. Audit and Consulting Services

- 4.1. a) The resume and b) job description for the internal auditor
- 4.2. a) Audit standards, b) schedules and c) programs for IT and EC activities.
- 4.3. a) Internal and b) external audit reports issued within the past eighteen months, c) including management responses and evidence of corrective actions.
- 4.4. Copies of any a) internal or b) external reports related to penetration testing and intrusion detection.

Section 5. Vendor Management

- 5.1. Audit reports (e.g. SAS70) from vendors of core business systems, including all E-Commerce systems
- 5.2. Evidence of the financial stability of primary IT/EC vendors.
- 5.3. Vendor contracts and service agreements.
- 5.4. Outline participation in user groups, advisory councils, etc.
- 5.5. Performance reports and logs of member service calls

Section 6. Member Service and Support

- 6.1. Incident reporting logs and reports.
- 6.2. Member help documentation for E-Commerce applications

Section 7. Personnel

- 7.1. a) Training plans and b) profiles for IT personnel
- 7.2. Certification and other professional credentials possessed by staff
- 7.3. a) Employee development plans and b) succession plans

Section 8. System Architecture and Controls

- 8.1. Network Topology Diagram (Do not include actual IP addresses)
- 8.2. Hardware and Software inventory (Do not include individual Workstations)

Section 9. Security Controls

- 9.1. Inventory of Security hardware and software, including firewalls, intrusion detection, user access controls, encryption devices, secure modems, user authentication components, virus protection software, etc.
- 9.2. Copies of recent reports related to authentication and intrusion detection.
- 9.3. Access control logs showing addition, changes and deletion of user privileges, including evidence of periodic management review
- 9.4. Description of physical security controls for IT hardware and software.
- 9.5. Evidence of updates to virus protection and intrusion detection applications

Section 10. Business Continuity

- 10.1. Copy of the Disaster Recovery and/or Business Continuity Plan
- 10.2. Copies of reports related to tests of the Disaster Recovery/Business Continuity plans done within last 18 months
- 10.3. List of the backup tapes, disks, documentation, supplies, etc. kept at your off-premises storage facility
- 10.4. Copies of Disaster Recovery Plans and agreements with Service Providers

Section 11. Performance Monitoring

- 11.1. Reports related to E-Commerce usage and activity levels
- 11.2. Member feedback regarding E-Commerce applications.

E-Commerce Questionnaire (EC-1)

_____ Credit Union

Sec. #	Que. #	Sub. Que. #	Question	Yes/No/NA/ NR	Comments
1 General					
1	1	0	Does the credit union engage in e-Commerce activities with its members via the Internet, world-wide web, home banking, etc.		
1	2	0	Are e-Commerce products and services considered to be critical to the credit union's goals and strategies?		
1	3	0	Have adequate policies and procedures been developed for the credit union's e-Commerce activities?		
1	4	0	Does the credit union have an up-to-date e-Commerce organization chart or listing of key e-Commerce staff?		
1	5	0	Has management established an e-Commerce oversight committee comprised of representatives from applicable departments such as Marketing, Compliance, Operations, Information Systems, Security, and Audit (Note: Audit should be more of an observer function rather than a participant function in order to avoid a conflict of interest)?		
1	6	0	Have information systems strategies and long-term strategic and short-term tactical plans been formulated and approved by the Board of Directors to support the overall e-Commerce strategy and information systems requirements of the credit union?		
1	7	0	Does the credit union Board of Directors receive reports on e-Commerce activities on a regular basis?		
1	8	0	Is the best description of the website (select only one):		
1	8	1	Informational		
1	8	2	Interactive		
1	8	3	Transactional		
1	9	0	Is the website hosted by the:		
1	9	1	Credit Union		
1	9	2	Vendor		
1	9	3	Third Party		
1	10	0	Is the website content developed and maintained by the credit union?		

E-Commerce Questionnaire (EC-1)

_____ Credit Union

1 11 0 Does the credit union offer the following services electronically:

1	11	1	Member Application	
1	11	2	Share Account Application	
1	11	3	Share account transfers	
1	11	4	Loan Applications	
1	11	5	Loan payments	
1	11	6	Bill payment	
1	11	7	Account Balance Inquiry	
1	11	8	View Account History	
1	11	9	Download Account History	
1	11	10	Share Draft Orders	
1	11	11	Merchandise Purchase	
1	11	12	Electronic Cash	
1	11	13	Wire Transfers	
1	11	14	Other (describe)	

2 Risk Assessment

2	1	0	Are there policies, procedures and practices in place for performing risk assessments to identify internal and external threats and vulnerabilities associated with e-Commerce?	
2	2	0	Do these policies and procedures address Operational/Transactional, Security, Reputation, and Compliance Risks?	
2	3	0	Has a risk assessment been performed for the credit union's e-Commerce activities?	
2	4	0	Does management actively reevaluate risks associated with technological and operational changes in e-Commerce?	
2	5	0	Has management considered, and is it continually monitoring, the risks associated with outsourcing relationships?	

3 Compliance and Legal

3	1	0	Is legal counsel consulted for significant matters such as e-Commerce contracts, partnerships, and affiliations?	
---	---	---	--	--

E-Commerce Questionnaire (EC-1)

_____ Credit Union

3	2	0	Does management actively monitor applicable laws and regulations and update related policies and procedures accordingly?	
3	3	0	Have appropriate procedures been put in place to ensure that e-Commerce transactions are legally binding (e.g., verifiably performed by the appropriate party) and cannot be repudiated?	
3	4	0	Has management determined whether e-Commerce activities are included in its bond coverage and, if so, has management determined if the coverage is sufficient?	
3	5	0	Does management review the credit union's bond coverage annually to ensure that it is adequate in relation to the potential risk?	
3	6	0	Has management considered the legal ramifications associated with providing e-Commerce services to multi-state and multinational members?	
3	7	0	Does the credit union's website include a privacy statement?	
4 Audit and Consulting Services				
4	1	0	Are e-Commerce activities subject to periodic internal and/or external (SAS 70 or financial statement) audits and quality reviews?	
4	2	0	Has management prioritized the issues disclosed in the most recent audit or quality review?	
4	3	0	Has management corrected, or is in the process of correcting, these issues?	
4	4	0	Has management performed and documented an assessment to determine if Attack and Penetration Testing should be used as a means of identifying, isolating, and confirming possible flaws in network and security architecture?	
4	5	0	If the assessment warrants penetration testing, has management performed, contracted for, or planned to contract for, these services?	
4	6	0	If a penetration test has been performed, has management addressed, or is in the process of	

addressing, identified vulnerabilities?

5 Vendor Management

- 5 1 0 Has management assessed long-term strategic and short-term tactical plans for current and future e-Commerce outsourcing activities?
- 5 2 0 Does management actively monitor whether critical outsourced service providers continually meet the credit union's e-Commerce needs (i.e. hardware, software, network services)?

6 Member Service and Support

- 6 1 0 Does management have a process in place to adequately track and resolve member support issues (e.g., member technical support, incident reports, and FAQ's)?
- 6 2 0 Has management established and tailored member service level goals based on business needs, field of membership, and member expectations?

7 Personnel

- 7 1 0 Is the credit union adequately staffed and trained with respect to its e-Commerce strategy?
- 7 2 0 Does an adequate segregation of duties exist between conflicting e-Commerce related responsibilities?
- 7 3 0 Does the management have a process in place to handle the addition, modification, or deletion of employee's access due to status changes (i.e. terminations, transfers, promotions)?
- 7 4 0 Has management implemented practices to address the recruitment and retention of e-Commerce technical staff?

8 System Architecture and Controls

- 8 1 0 Are adequate network, system and application diagrams (i.e. topologies) maintained?
- 8 2 0 Is an adequate inventory of e-Commerce hardware and software maintained?

9 Security Controls

E-Commerce Questionnaire (EC-1)

_____ Credit Union

9	1	0	Does management have an adequate security program in place (i.e., documented policies and procedures) which addresses protecting critical data and facilities?	
9	2	0	Does management monitor credit union staff activity to ensure compliance with established security policies and procedures?	
9	3	0	Have safeguards been implemented to mitigate the risk of confidential member and servicing information being disclosed to, or modified by, unauthorized users?	
9	4	0	Have authentication techniques/controls been put in place to block unwanted communications into and out of the credit union network (i.e., Firewall)?	
9	5	0	Have member session controls been put in place to ensure that access is only granted to the appropriate users?	
9	6	0	Have controls been put in place that automatically log-off a session (member or other users) as a result of inactivity?	
9	7	0	Has management classified data based upon its sensitivity, perceived value, and the impact to the credit union in the event of its loss?	
9	8	0	Have the various types of data communicated on and through the credit union's network been categorized according to its sensitivity?	
9	9	0	Has management implemented adequate security policies and procedures according to the sensitivity and importance of data?	
9	10	0	Is a criteria in place which determines the level of encryption that shall be used for the varying degrees of sensitive information?	
9	11	0	Is an appropriate level of encryption being utilized to protect sensitive data (data residing on the webserver or transmitted during a session)?	
9	12	0	Are effective and thoroughly tested security tools used to monitor internal and external threats?	
9	13	0	Does management ensure that virus identification and protection software is implemented, monitored, and	

E-Commerce Questionnaire (EC-1)

_____ Credit Union

updated when required?

- | | | | |
|---|----|---|---|
| 9 | 14 | 0 | Does the credit union have an intrusion detection system? |
| 9 | 14 | 1 | If yes, is it a real-time intrusion detection system? |
| 9 | 16 | 0 | Does management respond to potential intrusions in a timely manner? |

10 **Business Continuity**

- | | | | |
|----|---|---|---|
| 10 | 1 | 0 | Has disaster recovery relating to e-Commerce been incorporated into the credit union's overall business continuity plan? |
| 10 | 2 | 0 | Does management review its plan, at least annually, based on changes in technology, its infrastructure, or e-Commerce activities? |
| 10 | 3 | 0 | Is the plan tested on a regular basis and are the test results analyzed to identify necessary changes? |
| 10 | 4 | 0 | Has management developed incident response and escalation procedures for technical, security, or member concerns? |

11 **Performance Monitoring**

- | | | | |
|----|---|---|--|
| 11 | 1 | 0 | Has management established and implemented adequate performance monitoring procedures for e-Commerce activities? |
| 11 | 2 | 0 | Does management monitor the performance of e-Commerce activities against long-term and short-term plans, or member demands and expectations? |